APPENDIX B

March 15, 2004

[Section X] Functional Criterion for Table A.[1]

(a) Standard. A technology may be added to Table A upon a determination pursuant to [insert appropriate procedural regulation] that the technology – together with associated terms and conditions affecting security (including output and recording control, enforcement, and Change Management) that must be implemented as a strict condition of using the technology in devices – provides Affirmative and Reasonable Constraints on the digital redistribution of Marked and Unscreened Content through the digital outputs and connections of a Covered Product beyond the Local Environment of such Covered Product. For these purposes, "digital redistribution" does not include the physical movement of portable media or devices on which such content has been recorded. Thus, the technology need not impose any restrictions on such physical movement, so long as recording and playback are compliant with this subpart.

(b) Definitions.

(1) "Affirmative Constraints" means constraints that include each of the requirements of subsection (c) below and that effectively prevent digital redistribution beyond the Local Environment.

(2) "Local Environment" is the set of compliant, authorized devices within a tightly defined geographic area around a product. Mechanisms to define the Local Environment consist of: A) controls to limit distance from such product, B) limits on the scope of the network addressable by such product, and C) affinity-based controls used to approximate association of such set of devices with an individual or household. For example, the Local Environment of a product in a home consists of the set of authorized devices within or in the immediate vicinity (e.g., the yard, garage, or driveway) of that home but does not include products or devices located in a neighbor's home or operated by passers-by. Devices in an individual's car, RV, or boat are considered to be in the Local Environment of a product that is in an individual's home when the devices are in the immediate vicinity of that individual's home.

(3) "Reasonable Constraints" means constraints that in the normal course of operation prevent digital redistribution beyond the Local Environment.

---

[1] This model would also add appropriate procedural and other extensions to various of the provisions submitted by the MPAA *et al.* in connection with its proposal for Marketplace Criteria in Appendix A of our initial Comments to this FNPRM. Most importantly, Sections X.20(c) (information to be included in applications), X.21(c) (conditions of grant of application), X.21(c)(1)(D) (output and recording controls in license), X.21(c)(8) (intellectual property disclosure and obligations), and X.23(b) (withdrawal of authorization) would be adjusted accordingly.

(c) Mandatory Characteristics. To be considered for Table A under this criterion, a technology (and its associated terms and conditions) may be implemented – subject to the terms of applicable agreements – in hardware or software or both and must include in each case each of the following characteristics. Compliance with this section is a threshold requirement and does not determine that a technology must or should be added to Table A.

(1) the technology must effectively encrypt the content using cryptographic ciphers and cryptosystems of appropriate strength, key length, and in a manner such that:

(A) all cryptographic algorithms (including but not limited to symmetric and asymmetric ciphers, one-way cryptographic hashes, and cryptographic random number generators) shall have undergone public peer review and achieved widespread, published acceptance within the cryptographic scientific community to be strong algorithms;

(B) all cryptographic algorithms shall be such that detailed knowledge of the algorithms, the implementation of the algorithms, or both shall not, in and of itself, be sufficient information to allow the development or production of circumvention devices;

(C) all cryptographic algorithms, cryptosystems, keys and secrets shall be of sufficient strength, bit length, and implementation structure to render cryptanalysis to be computationally infeasible and prevent a system breach or compromise of content within the reasonably foreseeable future taking into account anticipated increases in processor speed/computational power, the possibility of distributed attacks, and future cryptanalysis techniques;

(2) the technology must utilize an authentication method such that any device participating in the exchange of Unscreened Content or Marked Content must:

(A) determine the authenticity of target sink device(s) on a regular and frequent basis prior to transmitting the content, including but not limited to confirming such sink device's existence in the Local Environment of the sending device. "Authenticity" means that the sink device demonstrates secure credentials showing it is authorized to implement the technology.

(B) securely manage the communication and distribution of any cryptographic keys and any secrets for decrypting the content using specific means to restrict such communication and distribution to within the Local Environment of the sending device;

(C) use specific means to limit exchanges of content beyond the Local Environment of the sending device, such as, but not limited to, Round Trip Time (RTT) limits; provided that use of any particular means may be found to be insufficient to meet this Mandatory Characteristic due to known or likely techniques for capturing and transmitting content beyond the Local Environment; and

(D) use specific affinity-based mechanisms, such as, but not limited to, password protection, user registration and/or cryptographic domain binding, in order to approximate association of a set of devices within a Local Environment with an individual or household and constrain content exchanges to those devices;

(3) decryption of such authenticated, encrypted transmission must be licensed, and such licenses must impose as terms and conditions the Compliance Rules of Subpart M and robustness requirements that comply with the Robustness Rules of [Section Y] on the sink device; provide content owners with an opportunity to meaningfully object to amendments to the license; and assure that such terms and conditions are imposed on all subsequent receiving devices;

(4) the technology must be implemented in Covered Demodulator Products and Peripheral TSP Products in hardware and software in a robust manner that complies with the Robustness Rules provided in Section [Y] below;

(5) the technology must incorporate an effective mechanism for revoking any lost, stolen, intercepted or otherwise misdirected cryptographic key or keys associated with a particular device; and any key or keys that are associated with a particular device and that have been made public or disclosed in violation of a license agreement, or cloned without authorization of the entity generating and licensing the keys. ("Key" includes any associated device identity or certificate or the like.)

(6) if the technology is implemented in software or upgradeable firmware, it must support a secure mechanism for system renewability and upgradeability in order to restore the content protection capabilities of the technology in the case of a successful system attack.

(d) Other Considerations.

(1) In making a determination of whether a proposed technology together with its terms and conditions does provide Affirmative and Reasonable Constraints on the ability of Covered Products to digitally redistribute Marked Content and Unscreened Content through the digital outputs and connections of Covered Products beyond the Local Environment of the sending device, in addition to the Mandatory Characteristics set forth above, the following shall also be considered:

(A) the capabilities of the technology to constrain digital redistribution addressing both present and foreseeable threats that may be envisioned at the time of such determination; hence, the addition of any technology to Table A under this criterion or the existence of any Technology on Table A under any other criterion is not a significant factor in assessing a newly proposed technology, although the failure of a proposed technology to implement characteristics of prior Table A technologies can be a significant factor militating against addition of the new technology to Table A;

(B) the geographic reach of possible dispersal of a signal at usable strength (i) absent the intervention of typical barriers such as walls within and surrounding a home, and (ii) in the face of such barriers;

(C) geographic limits, if any, imposed by need for, possible use of, or absence of physical carriers, such as wires and cable, and relevance of proximity features such as distance and sight lines, provided that any need for, use and relevance of such physical carriers or proximity features may be found to be of little or no weight in the face of encapsulation, tunneling, or other techniques for capturing and transmitting content beyond the Local Environment of a Covered Product; and

(D) the extent to which the proposed technology prevents or deters access to encrypted content by unauthorized devices including non-targeted sinks on the same network (i.e., "snooping").

(2) For the purpose of this criterion, the mere implementation of device counting, unaccompanied by substantial other characteristics in addition to those required by subsection (c), is not an Affirmative or Reasonable Constraint.

[Section Y] Robustness Requirements.

(a) In General. These robustness rules apply to the construction and implementation of Table A Technologies in Covered Products and Downstream Products and the behavior of such products with regard to the handling of Unscreened Content, Marked Content, and Downstream Content. For the purpose of these rules: (i) "Covered Products" include Covered Demodulator Products and Peripheral TSP Products; (ii) a "Downstream Product" is a product other than a Covered Product that receives content from a Table A Technology or from a technology that is approved for output or recording Downstream Content, including Downstream Content from a prior Downstream Product or from a succession of products that are linked by transmission from an initial Covered Product; (iii) "Downstream Compliance Requirements" are requirements of initial and subsequent Downstream Products that replicate the conditions of Subpart M under licenses for Table A Technologies as required under Section [X](c)(3) of the Functional Criteria; and (iv) "Downstream Content" is content that originated as Unscreened or Marked Content in a Covered Product and that is received by an initial or subsequent Downstream Product. Without limitation, Demodulator and Downstream Compliance Requirements include features and conditions pertaining to implementation of the Table A technology, such as encryption and decryption functions, and to related requirements such as avoidance of unprotected and non-authorized outputs and of unprotected or unauthorized protection of recordings in Covered and Downstream Products. Unless the sense of a provision is to the contrary, references to "Table A Technology" shall include any technology that is approved for recording Downstream Content in, or for output of Downstream Content from, a Downstream Product.

(1) Table A technologies shall be implemented in Covered and Downstream Products in a manner clearly designed to effectively frustrate attempts to modify such technologies to defeat the Demodulator Compliance Requirements and Downstream Compliance Requirements.

(2) Table A technologies and Covered and Downstream Products shall not include:

(A) switches, buttons, jumpers or software equivalents thereof,

(B) exposed traces, pins, or vias (i.e., only buried traces, hidden pins and hidden vias are allowed), or

(C) functions (including service menus and remote-control functions),

in each case by which the Demodulator or Downstream Compliance Requirements can be defeated, or by which compressed unencrypted Marked Content, compressed unencrypted Unscreened Content, or compressed unencrypted Downstream Content can be exposed to output, interception, retransmission, or copying, in each case other than as permitted under Subpart M or similar Downstream Compliance Requirements.

(3) Table A technologies shall be implemented in Covered and Downstream Products in a manner that is clearly designed to effectively frustrate attempts to discover or reveal any secret keys or secret algorithms used to meet the requirements of the Demodulator or Downstream Compliance Requirements.

(b) Data Paths. Within a Covered and Downstream Product, features including but not limited to implementations of Table A technologies shall not allow Unscreened Content, Marked Content, or Downstream Content to be present on any User Accessible Bus in unencrypted, compressed form.

(1) Uncompressed Content. During a petition opportunity that the Commission may designate, an interested person may petition the Commission to initiate a Notice of Inquiry to determine whether it is technically feasible and commercially reasonable to require that Unscreened Content, Marked Content or Downstream Content when transmitted over any User Accessible Bus in uncompressed digital form be made reasonably secure from unauthorized interception by using means that meet the standards set forth in Section [Y](d). Such petition shall include evidence that such an inquiry is warranted in light of generally available technologies and existing commercial circumstances. Should the Commission, based on such evidence and on consultation with affected industries, proceed with such Notice of Inquiry and thereby determine that requiring such protection at such level is technically feasible and commercially reasonable, the Commission may, pursuant to a Notice of Proposed Rulemaking, revise this Section to so require. The Commission will consider in its analysis: the general availability of relevant technologies, cost of implementation, effectiveness of any solutions, availability of alternative solutions, intellectual property licensing issues, consistency with requirements of other content protection systems, likely ability of manufacturers to satisfy the Robustness Requirements, and normal design cycles for such products. The Commission will exercise its discretion to limit the frequency of such Notices of Proposed Rulemaking. The procedures of this subparagraph shall apply as well to other provisions of these Robustness Rules that are currently limited to compressed content.

(c) Methods of Making Functions in Table A Technologies Robust. Table A technologies and other features in Covered and Downstream Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

(1) Distributed Functions. Where compressed Unscreened Content, compressed Marked Content, or compressed Downstream Content is delivered from one portion or implementation of the Table A technology or a Covered or Downstream Product to another portion or implementation of such Table A technology or such product , whether among integrated circuits, software modules, a combination thereof, or otherwise, such portions shall be designed and manufactured in a manner associated and otherwise integrated with each other such that such Unscreened Content, Marked Content, or Downstream Content as the case may be, in any usable form flowing between such portions of such Table A technology ore products shall be reasonably secure from being intercepted or copied except as permitted under the Demodulator and Downstream Compliance Requirements.

(2) Software. Without limiting the requirements of Sections [Y](a) and (b), portions of a Table A technology or Downstream or Covered Product that implement in Software the content protection requirements set forth in the Demodulator or Downstream Compliance Requirements shall:

(A) Comply with Section [Y](a)(3) by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode (i.e. in kernel mode), and/or embodiment in a secure physical implementation; and, in addition, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

(B) Be designed so as to perform or ensure checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide access to unencrypted Unscreened Content , unencrypted Marked Content, or unencrypted Downstream Content. For purposes of this Section [Y](c)(2)(B), a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections [Y](a) and (b). This Section [Y](c)(2)(B) requires at a minimum the use of signed code or more robust means of "tagging" operating throughout the code. For purposes of this Section [Y](c)(2), "signed code" means a method of achieving trusted distribution of Software by using public key cryptography, keyed hash, or other means at least as effective, to form a digital signature over Software such that its authenticity and integrity can be verified.

(3) Hardware. Without limiting the requirements of Sections [Y](a) and (b), the portions of a Table A technology or Downstream or Covered Product that implement in Hardware the content protection requirements set forth in the Demodulator or Downstream Compliance Requirements shall:

(A) Comply with Section [Y](a)(3) by any reasonable method including but not limited to (i) embedding any secret keys or secret cryptographic algorithms used to meet the content protection requirements set forth in the Demodulator Downstream Compliance Requirements in silicon circuitry or firmware that cannot reasonably be read or (ii) employing the techniques described above for Software.

(B) Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the security afforded by the requirements set forth in the Demodulator and Downstream Compliance Requirements would pose a serious risk of rendering the Table A technology or Covered or Downstream Product unable to receive, transmit, record, or play back Unscreened Content. Marked Content, and Downstream Content. By way of example, a component that is soldered rather than socketed, or affixed with epoxy, may be appropriate for this means.

(4) Hybrid. The interfaces between Hardware and Software portions of a Table A technologies and Covered and Downstream Products y shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection that would be provided by a pure Software implementation.

(d) Level of Protection. The content protection requirements set forth in the Demodulator and Downstream Compliance Requirements and the requirements set forth in Sections [Y](a)(3) and [Y](b) shall be implemented in a reasonable method so that they:

(1) Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons, or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers, other than Circumvention Devices; and

(2) Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section [Y](e)(1), such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

(e) Advance of Technology. Although an implementation of a Table A technology or other features of a Covered or Downstream Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design would have caused such products to fail to comply with this Section [Y] ("New Circumstances"). If a manufacturer implementing a Table A technology has actual notice or actual knowledge of New Circumstances that relate to the manufacturer's specific implementation of a Table A technology or other features of a Covered Demodulator Product (hereinafter referred to as "Notice"), then within 18 months after Notice such manufacturer shall cease distribution of such Covered Product or Downstream Product and shall only distribute Covered Products and Downstream Products that are compliant with this Section [Y] in view of the then-current circumstances.